

1

2 **ABSTRACT**

3 A method of decrypting a message encrypted using a truncated ring cryptosystem. The method
4 comprises selecting a window parameter T determining a plurality of windows of a
5 predetermined size, each window being shifted by an amount less than or equal to the window
6 parameter T. A decryption candidate is determined for each possible window. Each decryption
7 candidate is tested to determine whether it is a valid message. The result of the decryption is
8 chosen to be a valid message found in the previous step or if no valid message is found it is
9 indicated that the message could not be decrypted. By this method, a constant number of
10 decryption candidates are determined for each decryption.